INFOWATCH ARMA MANAGEMENT CONSOLE 1.6

What's new

Новые возможности

Подключение СЗИ внешних вендоров в качестве источников событий и сбор событий по CEF

Механизм обновления из веб-интерфейса и проверка пакета на безопасность

Разрыв сессии по тайм-ауту

Доступ к «Руководству пользователя» из интерфейса консоли

Карта сети

Уведомления

Экспорт по протоколу Syslog

Поиск и фильтрация в журналах

Расширение ролевой модели

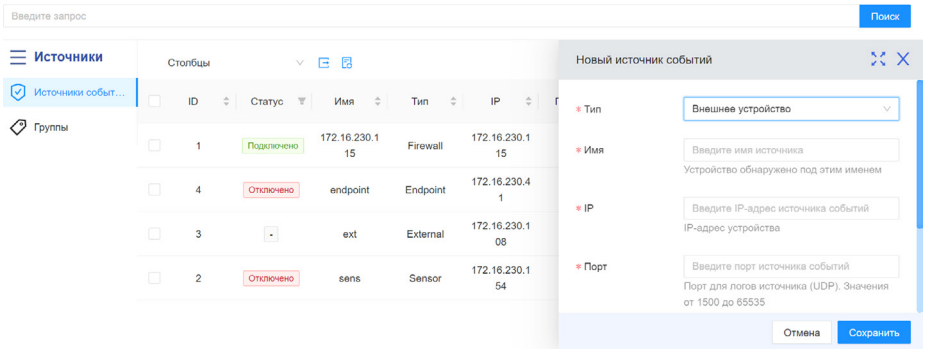
Обзорная панель с виджетами

Журнал действий пользователя

Подключение СЗИ внешних вендоров в качестве источников событий и сбор событий по CEF

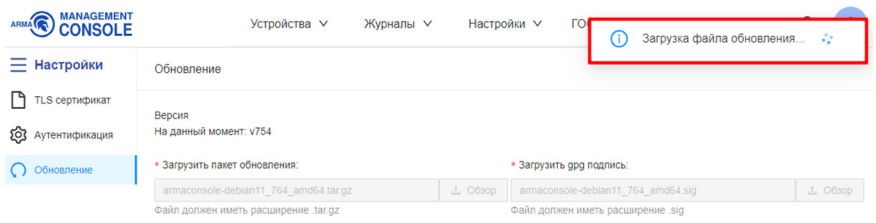
Появилась возможность добавить внешнее устройство (стороннего вендора) в качестве источника событий.

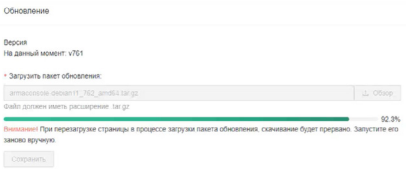
Новая функциональность позволит расширить возможности мониторинга и защиты инфраструктуры организации за счёт включения в анализ событий системы не только устройств InfoWatch ARMA, но и всех устройств в инфраструктуре компании, передающих события в формате CEF.



Механизм обновления из веб-интерфейса и проверка пакета на безопасность

Теперь загрузить обновлённую версию продукта можно непосредственно из интерфейса, не производя сложные манипуляции через терминальный консольный интерфейс.





Дополнительно: пакет проходит проверку на безопасность перед применением, статус загрузки обновления можно отслеживать в специальном окне

Разрыв сессии по тайм-ауту

Добавлена функция автоматического разрыва сессии доступа к интерфейсу консоли при неактивности пользователя более 15 минут. Для возобновления взаимодействия с интерфейсом потребуется повторная авторизация.

Данная функциональность удовлетворяет требованию УПД.10 приказа ФСТЭК России №239 — «Блокирование сеанса доступа пользователя при неактивности» — и позволяет повысить безопасность использования продукта.

Доступ к «Руководству пользователя» из интерфейса консоли

Появилась возможность перейти в руководство непосредственно из интерфейса, что упростит процесс поиска необходимой информации по продукту.

Карта сети

Возвращение и модификация возможностей версии 1.3

Стала доступна работа с сетевыми активами на карте сетевой инфраструктуры. В обновлённом разделе можно работать с основной картой, отображающей фактическое состояние сетевой инфраструктуры, а также создавать дополнительные карты и сохранять необходимые изменения, что позволит упростить управление сетевой инфраструктурой. В карте сети пользователь сможет:

- Выбирать активы, которые будут отображаться на сохранённой карте
- Видеть происходящие изменения в сетевой инфраструктуре
- Управлять изменениями в сохранённой карте
- Настраивать связи: связать активы или удалить связи
- Добавить картинку-подложку, чтобы визуализировать размещение активов
- Использовать возможности фильтрации: добавлен фильтр по активам с инцидентами для ускорения расследования инцидентов, групповой сброс фильтров, так же появилась возможность применения набора фильтров одновременно для упрощения поиска нужной информации
- Просматривать информацию по активу и перейти на произошедший инцидент непосредственно из карты сети

Рисунок 1. Выбор активов для сохранённой карты

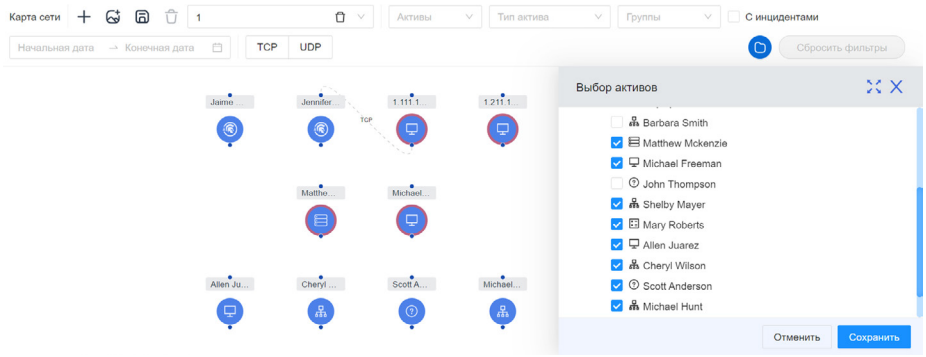


Рисунок 2. Отображение связей между устройствами сети

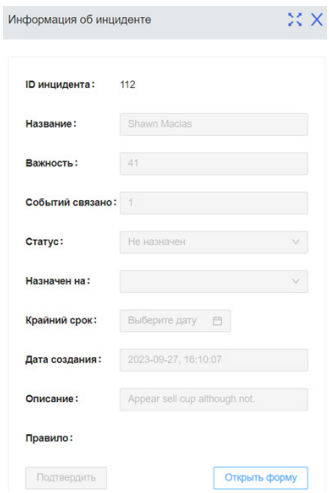
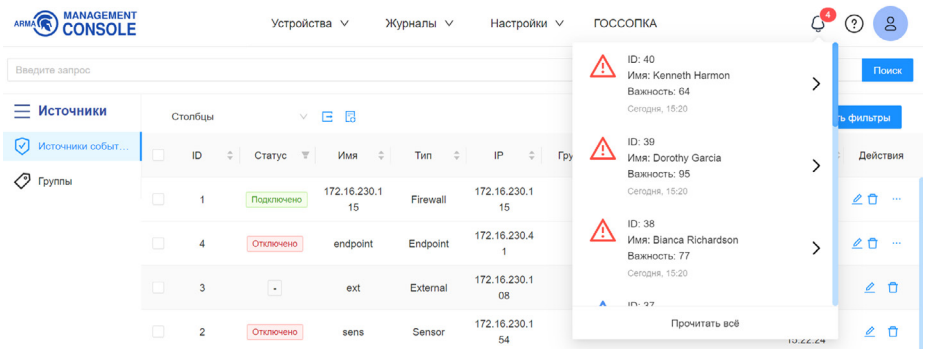


Рисунок 3. Информация об инциденте

Уведомления

Возвращение и модификация возможностей версии 1.3

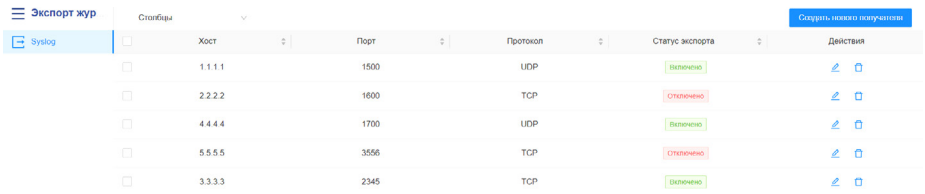
Благодаря уведомлениям можно увидеть информацию о произошедших инцидентах, находясь на любой странице интерфейса консоли. Это поможет оперативно реагировать на критичные изменения в инфраструктуре.



Экспорт по протоколу Syslog

Возвращение и модификация возможностей версии 1.3

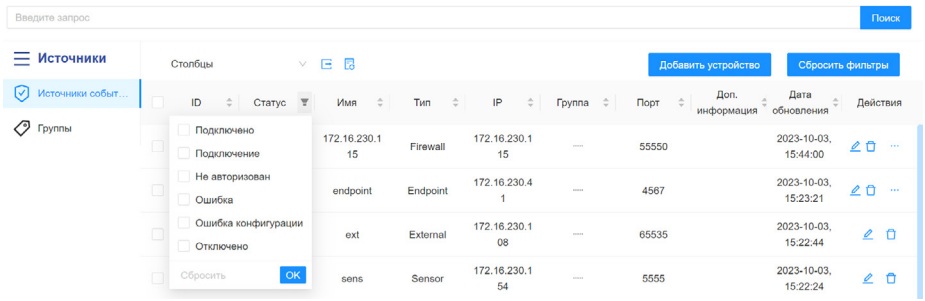
Стала доступна функция отправки событий в SIEM-системы сторонних производителей, что позволит расширить возможности мониторинга и защиты инфраструктуры организации.



Поиск и фильтрация в журналах

Возвращение и модификация возможностей версии 1.3

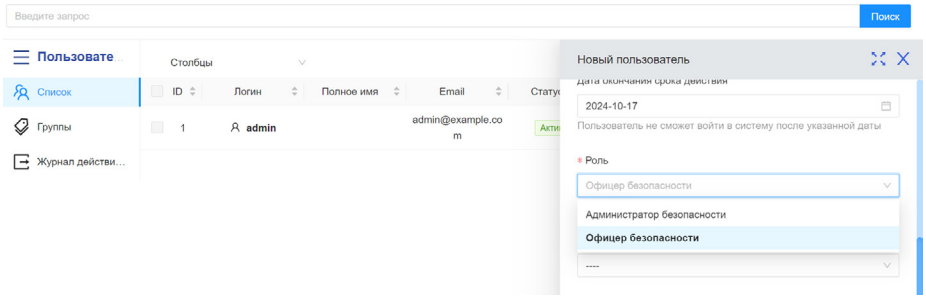
Поиск и фильтрация в журналах упростят процесс поиска нужной информации для проведения быстрой и качественной аналитики.



Расширение ролевой модели

Возвращение и модификация возможностей версии 1.3

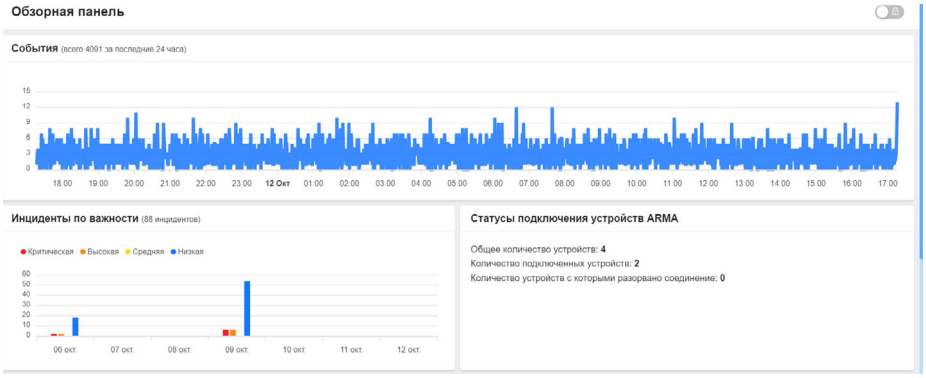
Добавлена роль «Офицер безопасности». Права доступа и привилегии теперь можно распределить между «Администратором» и «Офицером безопасности».



Обзорная панель с виджетами

Возвращение и модификация возможностей версии 1.3

Обновлён раздел Обзорной панели с изменённым составом виджетов — он позволяет ускорить мониторинг состояния ИБ и расследование инцидентов. Данные отображены в следующих виджетах: «Инциденты по важности», «Инциденты по группам», «Статусы подключения устройств», «Активы», «События».



Журнал действий пользователя

Позволит просмотреть информацию о всех действиях пользователей в системе, что увеличит прозрачность и повысит качество внутренней аналитики.